Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

M. Anderson Berry (*pro hac vice* forthcoming)
Gregory Haroutunian (*pro hac vice* forthcoming)
Brandon P. Jack (*pro hac vice* forthcoming)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: 916.239.4778
Fax: 916.924.1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

LINDA KAUFMAN, individually and on behalf of all others similarly situated, Plaintiff, v. NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	Case No. _____ CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiff Linda Kaufman ("Plaintiff" or "Kaufman"), individually and on behalf of all others similarly situated, brings this action against Defendants Northwell Health, Inc. ("Northwell") and Perry Johnson & Associates, Inc. ("PJA") (collectively, "Defendants"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from

Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Defendants' networks that resulted in unauthorized access to private health information. As a result of the Data Breach, Plaintiff and approximately 3.9 million Class Members[1] suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. Northwell is New York's largest healthcare provider, with hospitals in New York City, Long Island, and Westchester, including North Shore University Hospital and Long Island Jewish Medical Center. It has more than 900 hospitals and care centers, more than 85,000 employees, and more than 2 million patients per year.[2] PJA is a third-party vendor that provides medical transcription services including customized transcription solutions and coding, billing, recording, digital dictation, and court reporting services.[3]

3. Plaintiff and Class Members' sensitive personal information—which was entrusted to Defendants, their officials, and agents—was compromised and unlawfully accessed due to the Data Breach.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

[1] *See* https://www.hipaajournal.com/northwell-health-pja-data-breach/ (last visited November 17, 2023).
[2] *See* https://northwell.edu/about-northwell (last visited November 17, 2023).
[3] *See* Perry Johnson & Associates, Inc., BLOOMBERG, https://www.bloomberg.com/profile/company/ 0212500D:US#xj4y7vzkg (last visited November 17, 2023).

4. Information compromised in the Data Breach includes patient names in combination with their address, date of birth, Social Security number, medical record number, hospital account numbers, patient admission diagnoses, and likely other medical and treatment information held by Defendants, as a third-party vendor which maintained this information (collectively, "Private Information").

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained.

6. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus the Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Plaintiff and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information,

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial, medical, and other accounts to guard against identity theft.

10. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

13. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct, and asserting claims for: (i) negligence; (ii) negligence *per se*; and (iii) breach of implied contract.

14. Examples of the harms to the impacted individuals as a direct and foreseeable consequence of Defendants' conduct include the experiences of the representative Plaintiff, which are described below.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

16. This Court has personal jurisdiction over Defendant Perry Johnson & Associates, Inc. because it is a corporation incorporated under the laws of Nevada, has its principal place of business in Nevada, and does significant business in Nevada.

17. This Court has personal jurisdiction over Defendant Northwell Health, Inc., because it transacts business within this state and makes or performs contracts within this state.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because PJA has its principal place of business in Nevada, and a substantial part of the events giving rise to Plaintiff's claims arose in this District.

PARTIES

19. Plaintiff Linda Kaufman is a resident of Lawrence, New York. She is (and was during the period of the data breach) a citizen of the State of New York.

20. Defendant Northwell Health, Inc. is a corporation validly organized under the laws of New York with its principal place of business located at 480 W. 2000 Marcus Ave., New Hyde Park, NY 11042.

21. Defendant Perry Johnson & Associates is a Nevada corporation with its principal place of business at 1489 W Warm Springs Rd., Henderson, NV 89014. It may be served through its registered agent C T Corporation System, 701 S. Carson St., Suite 200, Carson City, NV 89701.

DEFENDANTS' BUSINESS

22. Northwell provides health care to more than 2 million individuals throughout the state of New York.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

23. On information and belief, in the ordinary course of rendering healthcare care services, Northwell requires patients to provide sensitive personal and private information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual and family medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Photo identification;
- Employment information, and;
- Other information that may be deemed necessary to provide care.

24. Additionally, Northwell may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, other doctors, patients' health plan(s), close friends, and/or family Members.

25. On information and belief, Northwell provides each of its patients with a HIPAA compliant notice titled "Privacy Policy" (the "Privacy Notice") that explains how it handles patients' sensitive and confidential information.

26. The Privacy Notice is provided to every patient upon request and is posted on Northwell's website.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

27. Because of the highly sensitive and personal nature of the information Defendants acquires and stores with respect to its patients, Northwell, upon information and belief, promises to, among other things: keep patients' protected health information; inform patients of its legal duties and comply with laws protecting patients' health information; only use and release patients' health information for approved reasons; and adhere to the terms outlined in the Privacy Policy.

28. As a condition of receiving treatment and services from Defendants, Defendants requires that all patients entrust it with highly sensitive personal information.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant Northwell assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' Private Information from unauthorized disclosure.

30. Defendant PJA provides medical transcription services to various healthcare organizations. Northwell used PJA for medical transcription and dictation services.

31. Plaintiff and Class members are current or former patients of Northwell and entrusted Northwell with their Private Information.

32. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

33. Plaintiff and the Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

THE CYBER ATTACK AND DATA BREACH

34. From March 27, 2023, and May 2, 2023, an unauthorized party gained and maintained access to Defendant PJA's network.[4] As a result of this access, an investigation occurred, and Defendant Northwell confirmed that patient data was exported and exfiltrated from the PJA network by this unauthorized party.[5]

35. The November 3, 2023 breach notice Plaintiff received from Defendant PJA on behalf of Defendant Northwell notes the types of Plaintiff's Private Information stolen in the Data Breach included her "name, date of birth, address, medical record number, hospital account number, and clinical information such as the name of the treatment facility, the name of your healthcare providers, admission diagnosis, dates and times of service, and files containing transcripts of operative reports, consult reports, history and physical exams, discharge summaries or progress notes, which may include the reason for your visit, your diagnoses, laboratory and diagnostic testing results, medical history including family medical history, surgical history, social history, medications, allergies, and/or other observational information."[6]

36. The investigation revealed that approximately a 3.9 million individuals were victims of the Data Breach.

37. Plaintiff's Private Information was compromised in the Data Breach. Plaintiff further believes her Private Information was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

---

[4] *See Notice of Data Breach* addressed to Plaintiff Kaufman dated November 3, 2023, attached hereto as **Exhibit A**.
[5] *Id.*
[6] *Id.*

38. Defendants had obligations created by HIPAA, contract, industry standards, common law, and their own promises and representations made to Plaintiff and Class Members that it would keep their Private Information confidential and protect it from unauthorized access and disclosure.

39. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

40. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

41. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

42. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

43. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[8]

---

[7] *See FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited November 17, 2023).

[8] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited November 17, 2023).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

44. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

Defendants Fail to Comply with FTC Guidelines

45. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[9] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

47. The FTC further recommends that companies not maintain personally identifiable information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested

[9] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last visited November 17, 2023).
[10] *Id*.

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750 lasvegas@stranchlaw.com

methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

50. Defendants failed to properly implement basic data security practices.

51. Defendants' failure to employ reasonable and appropriate measures to protect against and detect unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. Defendants were at all times fully aware of their obligation to protect the Private Information of patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Fail to Comply with Industry Standards

53. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

54. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

55. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

56. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

57. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Defendants' Conduct Violates HIPAA and Evidences Their Insufficient Data Security

58. The Health Insurance Portability and Accountability Act ("HIPAA") requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

59. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of Private Information. Safeguards must include physical, technical, and administrative components.

60. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

61. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because there is an access of private health information ("PHI") not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

62. Defendants' Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANTS' BREACH

63. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security systems to reduce the risk of data breaches and cyber-attacks;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to train their employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic Private Information that are not permitted under the privacy rules

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of their workforces effectively on the policies and procedures regarding Private Information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of Private Information, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic Private Information as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

p. Failing to adhere to industry standards for cybersecurity.

64. Defendants negligently and unlawfully failed to safeguard Plaintiff and Class Members' Private Information by allowing cyberthieves to access Defendants' computer network and systems which contained unsecured and unencrypted Private Information.

65. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendants.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Cyberattacks and Data Breaches Cause Disruption and Put Patients at an Increased Risk of Fraud and Identity Theft

66. Cyberattacks and data breaches at healthcare providers like Defendants are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

67. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[11]

68. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[12]

69. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[13]

70. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because

---

[11] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited November 17, 2023).

[12] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited November 17, 2023).

[13] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited November 17, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

71. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert, reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[14]

72. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

73. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may

[14] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/#/Steps (last visited November 17, 2023).

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

74. Moreover, theft of Private Information is also gravely serious, as it is an extremely valuable property right.[15]

75. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

76. Theft of private health information, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[16]

77. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed Private Information to adjust their insureds' medical insurance premiums.

---

[15] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[16] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited November 17, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

78. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

79. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

80. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

81. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

82. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

83. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[17] It is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

---

[17] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited November 17, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

84. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[18] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[19] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

85. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

86. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

87. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

[18] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited November 17, 2023).
[19] *Id* at 4.
[20] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited November 17, 2023).

to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[21]

88. Medical information is especially valuable to identity thieves, as the asking price for medical data on the black market typically can sell for $50 and up.[22]

89. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

90. For this reason, Defendants knew or should have known about these dangers and strengthened their data and systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet Northwell and PJA failed to properly prepare for that risk.

Plaintiff and Class Members' Damages

91. To date, Defendants have done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

92. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

93. Plaintiff's Private Information was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendants' computer network.

94. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

---

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited November 17, 2023).

[22] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited November 17, 2023).

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

95. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

96. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

97. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

98. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

99. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

100. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

101. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of Northwell's computer network and Plaintiff and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

102. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

103. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

104. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of the Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

105. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

Plaintiff Linda Kaufman's Experience

106. On or about November 3, 2023, Ms. Kaufman, a citizen and resident of Lawrence, New York, received Notice of Data Breach Letter by US. Mail.

107. As a patient of Northwell, she provided her Private Information to Defendants as part of their medical services, and under state and federal law, she was required to do so. She reasonably relied on Northwell, a sophisticated hospital and healthcare company, and its transcription service provider, PJA, to protect the security of her Private Information.

108. As a result of the Data Breach and the information that she received in the Notice Letter, Ms. Kaufman has spent many hours dealing with the consequences of the Data Breach (reviewing bank accounts, considering changing banks, changing passwords), as well as her time spent verifying the legitimacy of the Notice of Data Security Incident, exploring credit monitoring and identity theft insurance options, and other inconveniences. This time has been lost forever and cannot be recaptured.

109. Ms. Kaufman is very careful about sharing her own personal identifying information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

110. Ms. Kaufman stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

111. Ms. Kaufman suffered actual injury and damages due to Defendants' mismanagement of her Private Information before the Data Breach.

112. Ms. Kaufman suffered actual injury in the form of damages and diminution in the value of her Private Information —a form of intangible property that she entrusted to Defendants, which was compromised in and as a result of the Data Breach.

113. Ms. Kaufman suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered anxiety and increased concerns for the theft of her privacy since she received the Notice Letter.

114. Ms. Kaufman has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

115. Ms. Kaufman has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Northwell and PJA's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

116. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

117. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **All residents of the United States whose Private Information was compromised as a result of the Data Breach (the "Nationwide Class").**

118. Plaintiff also proposes the following New York Subclass definition, subject to amendment as appropriate:

> **All residents of New York whose Private Information was compromised as a result of the Data Breach (the "New York Subclass").**

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

119. The Nationwide Class and New York Subclass shall be hereinafter collectively referred to as the Class unless otherwise specified.

120. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which Defendants have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned, as well as his or her judicial staff and immediate family members.

121. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

122. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. While the total number of impacted individuals is unknown at this time, Northwell initially indicated that approximately 3.9 million patients were affected by the Data Breach.

123. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, inter alia:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' Private Information from unauthorized access and disclosure;

b. Whether Defendants had duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' Private Information;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

d. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' Private Information from unauthorized access and disclosure;

e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class members;

f. Whether Defendants breached their duties to protect Plaintiff's and Class members' Private Information; and

g. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

124. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

125. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her Private Information compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

126. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

127. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE
(on behalf of Plaintiff and the Class)

128. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

129. Defendants required patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of rendering healthcare services.

130. By collecting and storing this data in their computer property, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

131. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

132. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

133. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

134. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

135. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

136. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their systems had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

137. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

138. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

139. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

140. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT II
NEGLIGENCE *PER SE*
(on behalf of Plaintiff and the Class)

141. Plaintiff repeats and re-alleges each and every allegation contained the Complaint as if fully set forth herein.

142. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and the Class Members.

143. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Northwell and PJA, of failing to use reasonable measures to protect personal information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

144. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

145. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

146. Plaintiff and members of the Class are within the class of persons that the FTC Act was intended to protect.

147. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

148. As a direct and proximate result of Defendants' negligence per se, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information of current and former patients in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

149. Additionally, as a direct and proximate result of Defendants' negligence per se, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff and the Nationwide class)

150. Plaintiff repeats and re-alleges each and every allegation contained the Complaint as if fully set forth herein.

151. Plaintiff's and Class Members' Private Information was provided to Defendant Northwell as part of medical services that Defendant Northwell provided to Plaintiff and Class Members.

152. Plaintiff and Class Members agreed to pay Defendant Northwell for medical care and services.

153. Defendant Northwell and the Plaintiff and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' Private Information, whereby, Defendant Northwell was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' Private Information.

154. Defendant Northwell had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used in accordance with its contractual obligations.

155. Defendant Northwell was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' Private Information and to comply with industry standards and applicable laws and regulations for the security of this information.

156. Under these implied contracts for data security, Defendant Northwell was further obligated to provide Plaintiff and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

157. Defendant Northwell breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

158. Defendant Northwell further breached the implied contract by providing untimely notification to Plaintiff and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

159. The Data Breach was a reasonably foreseeable consequence of Defendant Northwell's actions in breach of these contracts.

160. As a result of Defendant Northwell's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain.

161. Had Defendant Northwell disclosed that its data security was inadequate, neither the Plaintiff or Class Members, nor any reasonable person would have entered into such contracts with Defendant Northwell.

162. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their Private Information, as well as the loss of control of their Private Information, and remain at present risk of suffering additional damages.

163. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

164. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant Northwell to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT IV
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§ 349, et seq.
(on behalf of Plaintiff and the New York Subclass)

165. Plaintiff repeats and re-alleges each and every allegation contained the Complaint as if fully set forth herein.

166. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New York Subclass Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and HITECH which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New York Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and HITECH;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New York Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and HITECH.

167. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

168. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff's and New York Subclass Members' rights. Data breaches within the healthcare industry put it on notice that its security and privacy protections were inadequate.

169. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

170. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the myriad New Yorkers affected by the Data Breach.

171. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

172. Plaintiffs and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a class action, defining the classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Classes requested herein;

b. Judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

d. An order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and,

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: November 21, 2023

Respectfully submitted,

/s/ Nathan R. Ring
Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, LLC
2100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102

M. Anderson Berry (*pro hac vice* forthcoming)
Gregory Haroutunian (*pro hac vice* forthcoming)
Brandon P. Jack (*pro hac vice* forthcoming)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: 916.239.4778
Fax: 916.924.1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com